14 Anneau des polynômes à une indéterminée

Dans l'ensemble de ce chapitre, $\mathbb{K}$ désigne l'un des corps $\mathbb{R}$ ou $\mathbb{C}$ [†].

1 Ensemble des polynômes à coefficients dans $\mathbb{K}$

1.1 Définition

Un polynôme est essentiellement défini par la donnée de la liste de ses coefficients. À titre d'exemple, le polynôme $4X^3 - 2X + 1$ est entièrement décrit par la liste $(1, -2, 0, 4)$. Une telle liste peut évidemment être arbitrairement longue, en lien avec le degré du polynôme considéré, mais aussi artificiellement complétée par des 0. Ainsi la liste $(1, -2, 0, 4, 0, 0)$ représente aussi le polynôme $4X^3 - 2X + 1 = 0X^5 + 0X^4 + 4X^3 + 0X^2 - 2X + 1$. Ces brèves observations conduisent naturellement à la définition suivante.

Définition 1 – Polynôme à une indéterminée à coefficients dans $\mathbb{K}$

- On appelle *polynôme (à une indéterminée) à coefficients dans* $\mathbb{K}$ toute suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang[‡], *i.e.* vérifiant
$$\exists n \in \mathbb{N}, \quad \forall k > n, \quad a_k = 0.$$
L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$ si l'on choisit de noter X l'*indéterminée* (notion qui sera précisée à la définition 7).
- Pour tout $k \in \mathbb{N}$, le terme a_k de la suite $(a_k)_{k\in\mathbb{N}}$ est appelé *coefficient (du terme) de degré k* du polynôme.

Conformément à cette définition, un polynôme est une suite de la forme $(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots)$ à coefficients dans $\mathbb{K}$. Nous pourrons bientôt noter $a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ une telle suite, notation qui nécessite toutefois d'être légitimée par ce qui va suivre. Il est cependant opportun d'avoir cet objectif en tête afin de comprendre les définitions qui vont suivre.

Quoi que l'on pense de la définition abstraite précédente, cette dernière a au moins le mérite de rendre trivial le résultat suivant. Son analogue pour les fonctions polynomiales étant autrement plus délicat à établir.

Théorème 2 – Identification des coefficients

Deux polynômes sont égaux si et seulement si leurs coefficients le sont.

Définition 3 – Polynôme constant, polynôme nul

On appelle *polynôme constant* de $\mathbb{K}[X]$ tout polynôme $(\lambda, 0, 0, \ldots)$, avec $\lambda \in \mathbb{K}$. Un tel polynôme sera simplement noté λ. Avec cette notation, le polynôme 0 est appelé *polynôme nul*.

1.2 Structure d'anneau

En vue de définir une addition et une multiplication sur $\mathbb{K}[X]$, nous aimerions pouvoir écrire
$$\left(\sum_{k=0}^{n} a_kX^k\right) + \left(\sum_{k=0}^{n} b_kX^k\right) = \sum_{k=0}^{n} (a_k + b_k)X^k$$
et
$$\left(\sum_{i=0}^{n} a_iX^i\right) \times \left(\sum_{j=0}^{n} b_jX^j\right) = \sum_{0\leqslant i,j\leqslant n} a_ib_jX^{i+j} = \sum_{k=0}^{2n} \overbrace{\left(\sum_{\substack{0\leqslant i,j\leqslant n\\ i+j=k}} a_ib_j\right)}^{\text{On regroupe les termes de même degré } k} X^k = \sum_{k=0}^{2n} \overbrace{\left(\sum_{i=0}^{k} a_ib_{k-i}\right)}^{\text{On élimine } j \text{ via la relation } j=k-i} X^k,$$

†. À l'exception notable du point **(i)** du théorème 27 et du théorème 33, l'ensemble des définitions et résultats de ce chapitre restent valables sur un corps $\mathbb{K}$ quelconque.

‡. Une telle suite est dite *presque nulle*.

avec, par convention, $a_i = b_i = 0$, pour tout $i > n$, où l'on reconnaîtra les règles usuelles du calcul littéral. Ces aspirations conduisent aux définitions suivantes.

Somme et produit de deux polynômes Si $P = (a_0, a_1, \dots, a_p, 0, 0, 0, \dots)$ et $Q = (b_0, b_1, \dots, b_q, 0, 0, 0, \dots)$ sont deux polynômes, il est clair que la suite $(a_k + b_k)_{k\in\mathbb{N}}$ est nulle à partir du rang $\max\{p, q\} + 1$ et définit donc un polynôme. La situation, moins immédiate pour le produit, est clarifiée par le lemme suivant.

Lemme 4 – Produit de Cauchy de deux suites presque nulles

- On appelle *produit de Cauchy*† de deux suites $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ la suite $(c_k)_{k\in\mathbb{N}}$ définie par

$$\forall k \in \mathbb{N}, \quad c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{\substack{0\leqslant i,j\leqslant k\\ i+j=k}} a_i b_j \tag{1}$$

- Si $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ sont deux suites presque nulles d'éléments de $\mathbb{K}$, alors leur produit de Cauchy $(c_k)_{k\in\mathbb{N}}$ l'est aussi. Précisément,

$$(\forall\, k > p, \quad a_k = 0 \quad \text{et} \quad \forall\, k > q, \quad b_k = 0) \quad \Longrightarrow \quad (\forall\, k > p+q, \quad c_k = 0 \quad \text{et} \quad c_{p+q} = a_p b_q).$$

Démonstration. ... ■

Nous sommes alors en mesure de définir une structure d'anneau sur l'ensemble $\mathbb{K}[X]$ des polynômes à une indéterminée à coefficients dans $\mathbb{K}$.

Définition-théorème 5 – Structure d'anneau sur $\mathbb{K}[X]$

Soit $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ deux éléments de $\mathbb{K}[X]$.

- On appelle *somme de P et Q*, notée $P + Q$, le polynôme $(a_k + b_k)_{k\in\mathbb{N}}$.
- On appelle *produit de P et Q*, noté $P \times Q$ ou PQ, le polynôme $\left(\sum_{i=0}^{k} a_i b_{k-i}\right)_{k\in\mathbb{N}}$. En particulier, pour tout $\lambda \in \mathbb{K}$, λP est le polynôme $(\lambda a_k)_{k\in\mathbb{N}}$.

Ces lois d'addition et de multiplication munissent l'ensemble $\mathbb{K}[X]$ d'une structure d'anneau commutatif.

Démonstration. La remarque liminaire de ce paragraphe montre que l'addition de deux polynômes définit une loi de composition interne sur $\mathbb{K}[X]$, qui est alors clairement un sous-groupe du groupe $\left(\mathbb{K}^{\mathbb{N}}, +\right)$, dont l'élément neutre est le polynôme nul 0. Par ailleurs, le lemme 4 montre que la multiplication de deux polynômes définit aussi une loi de composition interne sur $\mathbb{K}[X]$ et cette loi vérifie :

- *Commutativité.* La commutativité du produit découle de la symétrie en les coefficients a_i et b_j de la formule (1) du produit de Cauchy de deux suites.
- *Associativité.* Soit $P = (a_k)_{k\in\mathbb{N}}$, $Q = (b_k)_{k\in\mathbb{N}}$ et $R = (c_k)_{k\in\mathbb{N}}$ trois éléments de $\mathbb{K}[X]$. Le coefficient de degré $n \in \mathbb{N}$ de $P(QR)$ est
$$\sum_{i+l=n} a_i \left(\sum_{j+k=l} b_j c_k\right) = \sum_{i+j+k=n} a_i b_j c_k,$$
et l'on déduit par symétrie de cette expression, puis commutativité du produit, que
$$P(QR) = R(PQ) = (PQ)R.$$
- *Élément neutre.* Vérifions que $1 = (1, 0, 0, \dots) = \left(\delta_{k,0}\right)_{k\in\mathbb{N}}$ est l'élément neutre pour le produit.
Pour tout $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$, le coefficient de degré $k \in \mathbb{N}$ de $P \times 1$ est
$$\sum_{i=0}^{k} a_i \delta_{k-i,0} = a_k \delta_{0,0} = a_k.$$
- *Distributivité sur +.* Soit $P = (a_k)_{k\in\mathbb{N}}$, $Q = (b_k)_{k\in\mathbb{N}}$ et $R = (c_k)_{k\in\mathbb{N}}$ trois éléments de $\mathbb{K}[X]$. Le coefficient de degré $k \in \mathbb{N}$ de $P(Q+R)$ est
$$\sum_{i=0}^{k} a_i (b_{k-i} + c_{k-i}) = \sum_{i=0}^{k} a_i b_{k-i} + \sum_{i=0}^{k} a_i c_{k-i},$$
et l'on reconnaît la somme des coefficients de degré k de PQ et PR, ce qui établit $P(Q + R) = PQ + PR$. ■

✖ **Attention !** ✖ L'anneau $\mathbb{K}[X]$ n'est pas un sous-anneau de l'anneau $\mathbb{K}^{\mathbb{N}}$ des suites, la multiplication des polynômes étant définie via le produit de Cauchy des suites et non la multiplication terme à terme des suites.

†. Augustin Louis, baron Cauchy (1789 à Paris – 1857 à Sceaux) est un mathématicien français, membre de l'Académie des sciences et professeur à l'École polytechnique. Il introduit en analyse les fonctions holomorphes (fonction de la variable complexe) et des critères de convergence des suites et des séries entières. Ses travaux sur les permutations sont précurseurs de la théorie des groupes.

La structure d'anneau de $\mathbb{K}[X]$ permet alors de considérer les puissances d'un polynôme et on dispose bien sûr des règles de calcul classiques valables dans un anneau (théorèmes 18 et 59 du chapitre 11). En particulier, la formule du binôme et l'identité de Bernoulli s'appliquent sans restriction.

Corollaire 6 – Formule du binôme, Identité de Bernoulli

Pour tous $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$, $\quad (P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k} \quad$ et $\quad P^n - Q^n = (P-Q) \sum_{k=0}^{n-1} P^k Q^{n-k-1}$.

1.3 Notation définitive

Le temps de la notation polynomiale est enfin arrivé ! Désormais, grâce au théorème suivant, les polynômes seront toujours écrits selon notre conception intuitive initiale. Conformément au programme, il n'est pas illégitime d'oublier la construction qui précède. Le point de vue des suites presque nulles nous aura permis de définir proprement le monde des *polynômes formels à une indéterminée* – qualifiés ainsi pour les distinguer des fonctions polynomiales, sur lesquelles nous reviendrons plus tard.

Définition-théorème 7 – Notation polynomiale

Dans $\mathbb{K}[X]$, on choisit de noter X le polynôme $(0, 1, 0, 0, \ldots)$, appelé *indéterminée (formelle)*.

- Pour tout $k \in \mathbb{N}$, $\quad X^k = (\underbrace{0, \ldots, 0}_{k \text{ zéros}}, 1, 0, 0, \ldots) = (\delta_{j,k})_{j \in \mathbb{N}}$, polynôme pour lequel l'unique coefficient non nul vaut 1 et est en position « degré k », *e.g.*

$$1 = X^0 = (1, 0, 0, \ldots), \quad X = (0, 1, 0, 0, \ldots), \quad X^2 = (0, 0, 1, 0, 0, \ldots), \quad X^3 = (0, 0, 0, 1, 0, 0, \ldots), \quad \ldots$$

- On appelle *monôme* tout polynôme de la forme λX^k, où $\lambda \in \mathbb{K}$ et $k \in \mathbb{N}$.
- Pour tout polynôme $P = (a_0, \ldots, a_n, 0, 0, \ldots)$, on peut alors écrire $P = \sum_{k=0}^{n} a_k X^k$, écriture qui sous-entend que tous les coefficients de P sont nuls à partir du rang $n+1$.

Démonstration. L'égalité $X^k = (0, \ldots, 0, 1, 0, 0, \ldots)$, pour tout $k \in \mathbb{N}$, s'obtient par récurrence sur $k \in \mathbb{N}$. ■

Remarque 8 L'indéterminée formelle X n'est pas une variable (au sens fonctionnel), mais un polynôme bien précis, à partir duquel il est possible d'écrire les autres éléments de $\mathbb{K}[X]$. En particulier, l'indéterminée formelle ne doit pas être quantifiée et ne peut pas servir d'inconnue pour résoudre une équation.

✖ ATTENTION ! ✖ Attention, l'écriture $P = \sum_{k=0}^{n} a_k X^k$ ne sous-entend en aucune façon que $a_n \neq 0$!

Il convient donc *in fine* de retenir que les définitions de la somme et du produit de deux polynômes données à la définition-théorème 5 s'énoncent, pour tous $m, n \in \mathbb{N}$,

$$\sum_{k=0}^{m} a_k X^k + \sum_{k=0}^{n} b_k X^k = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) X^k \quad \text{et} \quad \sum_{k=0}^{m} a_k X^k \times \sum_{k=0}^{n} b_k X^k = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k = \sum_{\substack{0 \leqslant i \leqslant m \\ 0 \leqslant j \leqslant n}} a_i b_j X^{i+j}.$$

où, par convention, les a_k (resp. b_k) ne figurant pas dans l'écriture de $\sum_{k=0}^{m} a_k X^k$ (resp. $\sum_{k=0}^{n} b_k X^k$) sont nuls.

Remarque 9 Pour un polynôme $P = (a_k)_{k \in \mathbb{N}}$ à coefficients dans $\mathbb{K}$, on pourra aussi écrire $P = \sum_{k=0}^{+\infty} a_k X^k$ et cette écriture est unique. En dépit des apparences, une telle somme est FINIE, la suite $(a_k)_{k \in \mathbb{N}}$ des coefficients de P étant nulle à partir d'un certain rang. Cette notation « infinie » est parfois avantageuse pour la rédaction. Les formules pour la somme et le produit de deux polynômes rappelées précédemment se réécrivent alors

$$\sum_{k=0}^{+\infty} a_k X^k + \sum_{k=0}^{+\infty} b_k X^k = \sum_{k=0}^{+\infty} (a_k + b_k) X^k \quad \text{et} \quad \sum_{k=0}^{+\infty} a_k X^k \times \sum_{k=0}^{+\infty} b_k X^k = \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k = \sum_{i=0}^{+\infty} \sum_{j=0}^{+\infty} a_i b_j X^{i+j}.$$

Terminons cette première partie avec une application classique du théorème 2 d'identification des coefficients de polynômes.

Application 10 – Formule de Vandermonde Pour tout $n \in \mathbb{N}$, $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

2 Degré d'un polynôme

Pour un polynôme $P = \displaystyle\sum_{k=0}^{+\infty} a_k X^k$ non nul, l'ensemble $\{k \in \mathbb{N} \mid a_k \neq 0\}$ est une partie non vide et majorée de $\mathbb{N}$ (la suite $(a_k)_{k\in\mathbb{N}}$ des coefficients étant nulle à partir d'un certain rang), il admet donc un plus grand élément, ce qui légitime la définition suivante.

Définition 11 – Degré d'un polynôme, coefficient dominant, polynôme unitaire

- Soit $P = \displaystyle\sum_{k=0}^{+\infty} a_k X^k$ un polynôme à coefficients dans $\mathbb{K}$. On définit le *degré de* P, noté $\deg(P)$, par
$$\deg(P) = \begin{cases} \max\{k \in \mathbb{N} \mid a_k \neq 0\} & \text{si } P \neq 0 \\ -\infty & \text{si } P = 0. \end{cases}$$
- Lorsque P est non nul, le coefficient $a_{\deg P}$ de P est appelé son *coefficient dominant* et, lorsque ce dernier est égal à 1, le polynôme P est dit *unitaire*.
- L'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré INFÉRIEUR ou égal à n est noté $\mathbb{K}_n[X]$.

Exemple 12

- Le polynôme $P = 3X^2 - \sqrt{5}X + 2$ est de degré 2 et a pour coefficient dominant 3. Ainsi $P \in \mathbb{R}_2[X]$, mais on a aussi $P \in \mathbb{R}_{155}[X]$ par exemple, puisque $\deg P \leqslant 155$.
- Le polynôme $X^3 - 3X + 2$ est unitaire.

Remarque 13

- Un polynôme $\displaystyle\sum_{k=0}^{n} a_k X^k$ est de degré INFÉRIEUR ou égal à n, et est de degré n si et seulement si $a_n \neq 0$.
- Un polynôme est constant si et seulement s'il est nul ou de degré nul. Ainsi $\mathbb{K}_0[X]$ s'identifie à $\mathbb{K}$.

Théorème 14 – Degrés d'une somme et d'un produit

Soit $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

(i) Degré d'une somme. $\deg(P+Q) \leqslant \max\{\deg P, \deg Q\}$, avec égalité lorsque $\deg P \neq \deg Q$.

(ii) Degré d'un produit. $\deg(PQ) = \deg P + \deg Q$. En particulier, si $\lambda \neq 0$, $\deg(\lambda P) = \deg P$.

Démonstration. ... ■

Exemple 15 L'inégalité pour la somme est due à la situation suivante : si $P = X^2 + 1$ et $Q = -X^2 + X - 2$, alors $P + Q = X - 1$ et $\deg(P+Q) = 1 < \max\{\deg P, \deg Q\} = 2$.

Remarque 16

- Pour tous $\lambda, \mu \in \mathbb{K}$ et $P, Q \in \mathbb{K}[X]$, $\deg(\lambda P + \mu Q) \leqslant \max\{\deg P, \deg Q\}$.
- D'après le deuxième point du lemme 4, le coefficient dominant d'un produit de polynômes est le produit des coefficients dominants des facteurs du produit.

Corollaire 17

Pour tout $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ est stable par combinaison linéaire. En particulier, $\mathbb{K}_n[X]$ est un sous-groupe de $\mathbb{K}[X]$.

✖ **ATTENTION !** ✖ En revanche, $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$, dès que $n \geqslant 1$. En effet, $(X^n)^2 \notin \mathbb{K}_n[X]$.

Corollaire 18 – Intégrité de $\mathbb{K}[X]$

L'anneau $\mathbb{K}[X]$ est *intègre*, *i.e.* vérifie

$$\forall P, Q \in \mathbb{K}[X], \quad PQ = 0 \implies (P = 0 \text{ ou } Q = 0).$$

Démonstration. Soit $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$. Alors $\deg P + \deg Q = \deg(PQ) = -\infty$ et nécessairement $\deg P = -\infty$ ou $\deg Q = -\infty$, *i.e.* $P = 0$ ou $Q = 0$. ∎

Remarque 19 Cette propriété serait nettement plus difficile à prouver si l'on travaillait avec des fonctions polynomiales et non avec des polynômes. En effet, si $P(x)Q(x) = 0$, pour tout $x \in \mathbb{R}$, alors en tout point l'une des fonctions P ou Q s'annule, mais rien ne nous garantit alors que l'une des deux s'annule tout le temps.

Corollaire 20 – Inversibles de $\mathbb{K}[X]$

Les éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes de degré 0, *i.e.* $\mathrm{U}(\mathbb{K}[X]) = \mathbb{K}^*$.

Démonstration.

- Si P est un polynôme de degré 0, *i.e.* une constante non nulle λ, alors λ^{-1} (inverse de λ dans $\mathbb{K}$) est l'inverse de P.
- Soit $P \in \mathrm{U}(\mathbb{K}[X])$, il existe alors $Q \in \mathbb{K}[X]$ tel que

$$PQ = 1 \implies 0 = \deg 1 = \deg(PQ) = \deg P + \deg Q \implies \deg P = 0,$$

puisque $\deg P, \deg Q \in \mathbb{N} \cup \{-\infty\}$. ∎

3 Composition et dérivation des polynômes

Définition-théorème 21 – Composition des polynômes

Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ et Q deux éléments de $\mathbb{K}[X]$.

- On appelle *composée de Q suivie de P*, notée $P \circ Q$ ou $P(Q)$, le polynôme

$$P \circ Q = \sum_{k=0}^{+\infty} a_k Q^k.$$

- **Degré d'une composée.** Si Q n'est pas constant, alors $\deg(P \circ Q) = \deg P \times \deg Q$.

Démonstration. Supposons Q non constant et posons $m = \deg P$. Par produit, $\deg\big(Q^k\big) = k \deg Q$, pour tout $k \in [\![0\,,m]\!]$. Ainsi, puisque $\deg Q \geqslant 1$, la suite $\big(\deg(Q^k)\big)_{0 \leqslant k \leqslant m}$ est strictement croissante. Finalement, par somme,

$$\deg(P \circ Q) = \deg\left(\sum_{k=0}^{m} a_k Q^k\right) \underset{a_m \neq 0}{=} \deg(Q^m) = m \deg Q.$$

∎

Remarque 22

- Si Q est constant, *i.e.* un élément de $\mathbb{K}$, on peut avoir $P \circ Q = 0$, *i.e.* Q est une racine de P, avec $PQ \neq 0$, auquel cas l'égalité $\deg(P \circ Q) = \deg P \times \deg Q$ n'est pas vérifiée.
- Comme pour les puissances d'un nombre, pour tout $Q \in \mathbb{K}[X]$, $Q^0 = 1$, on a donc pour $P = \sum_{k=0}^{n} a_k X^k$:

$$P \circ Q = a_n Q^n + a_{n-1} Q^{n-1} + \ldots + a_2 Q^2 + a_1 Q + a_0.$$

- Dans le cas particulier où $Q = X$, le polynôme $P(Q) = P(X)$ est égal à P, c'est pourquoi on utilise aussi bien l'écriture P que $P(X)$ pour désigner ce polynôme.
- On peut montrer sans difficulté que, pour tous $\lambda, \mu \in \mathbb{K}$ et $P, Q, R \in \mathbb{K}[X]$,

$$(\lambda P + \mu Q) \circ R = \lambda P \circ R + \mu Q \circ R \qquad \text{et} \qquad (PQ) \circ R = (P \circ R) \times (Q \circ R).$$

Exemple 23

- Un polynôme P est dit *pair* lorsque $P(-X) = P(X)$.

  Or si $P = \sum_{k=0}^{+\infty} a_k X^k$, alors $P(-X) = \sum_{k=0}^{n} (-1)^k a_k X^k$. Ainsi P est pair si et seulement si, pour tout $k \in \mathbb{N}$, $a_{2k+1} = 0$, *i.e.* si et seulement si P est combinaison linéaire de puissances paires de X.
- Similairement, un polynôme P est dit *impair* lorsque $P(-X) = -P(X)$. Ainsi P est impair si et seulement s'il est combinaison linéaire de puissances impaires de X.

Définition 24 – Dérivation des polynômes

Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$.

- Le polynôme $\sum_{k=1}^{+\infty} k a_k X^{k-1}$ est appelé le *polynôme dérivé de* P et noté P'.
- On définit par récurrence, pour tout $r \in \mathbb{N}$, le r^e *polynôme dérivé de* P, noté $P^{(r)}$, $\begin{cases} P^{(0)} = P, \\ \forall r \in \mathbb{N}, \quad P^{(r+1)} = \left(P^{(r)}\right)'. \end{cases}$

  Pour $r \in \{2,3\}$, on préfère toutefois les notations P'' et P''' à $P^{(2)}$ et $P^{(3)}$.

La définition précédente est évidemment basée sur les propriétés bien connues de dérivation des fonctions polynomiale sur $\mathbb{R}$. Toutefois, il s'agit ici d'une définition purement formelle de la notion de dérivée, nullement adossée à un concept de limite dans $\mathbb{K}[X]$. En particulier, dans le contexte des polynômes formelles, il est parfaitement hors de propos de s'intéresser à la dérivabilité.

Exemple 25 Pour $P = 8X^3 - 5X^2 + 3X + 1$, on a

$$P' = 24X^2 - 10X + 3, \qquad P'' = \left(P'\right)' = 48X - 10, \qquad P''' = \left(P''\right)' = 48, \qquad P^{(4)} = \left(P'''\right)' = 0$$

et donc $P^{(r)} = 0$, pour tout $r \geqslant 4$.

Exemple 26 Pour tous $n \in \mathbb{N}$ et $p \in [\![0\,,n]\!]$, $\quad (X^n)^{(p)} = n(n-1)\cdots(n-p+1)X^{n-p} = p!\dbinom{n}{p}X^{n-p}$.

Les règles opératoires pour la dérivation des polynômes formelles sont identiques à celles pour les fonctions dérivables !

Théorème 27 – Propriétés de la dérivation des polynômes

Soit $P, Q \in \mathbb{K}[X]$, $\lambda, \mu \in \mathbb{K}$ et $r \in \mathbb{N}$.

(i) Degré. $\begin{cases} \deg\left(P^{(r)}\right) = \deg P - r & \text{si } r \leqslant \deg P, \\ P^{(r)} = 0 & \text{sinon.} \end{cases}$ En particulier, P est constant si et seulement si $P' = 0$.

(ii) Linéarité. $(\lambda P + \mu Q)^{(r)} = \lambda P^{(r)} + \mu Q^{(r)}$.

(iii) Produit. $(PQ)' = P'Q + PQ'$ et plus généralement

$$(PQ)^{(r)} = \sum_{k=0}^{r} \binom{r}{k} P^{(k)} Q^{(r-k)} \qquad \textit{(formule de Leibniz}^{\dagger}\textit{)}.$$

(iv) Composition. $(P \circ Q)' = Q' \times P' \circ Q$.

Démonstration. ... ■

Remarque 28 À l'instar des fonctions, la formule de dérivation d'un produit se généralise à un produit d'un nombre fini quelconque de facteurs :

$$\forall P_1, \ldots, P_n \in \mathbb{K}[X], \qquad \left(\prod_{i=1}^{n} P_i\right)' = \sum_{i=1}^{n} P_i' \prod_{j \neq i} P_j.$$

✖ **Attention !** ✖ La relation $\deg P' = degP - 1$ est fausse pour un polynôme P constant.

†. Gottfried Wilhelm Leibniz (1646 à Leipzig – 1716 Hanovre), est un philosophe, scientifique, mathématicien, logicien, diplomate, juriste, bibliothécaire et philologue allemand. On lui attribue généralement, avec Isaac Newton, l'invention du calcul infinitésimal.

Exercice 29 Pour tous $n \in \mathbb{N}$ et $p \in [\![0\,,n]\!]$, $\left((aX+b)^n\right)^{(p)} = a^p p! \binom{n}{p} (aX+b)^{n-p}$.

4 Évaluation d'un polynôme

4.1 Fonction polynomiale associée

Définition-théorème 30 – Évaluation polynomiale, fonction polynomiale associée

Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un élément de $\mathbb{K}[X]$.

- Pour tout $\alpha \in \mathbb{K}$, on définit $P(\alpha) = \sum_{k=0}^{+\infty} a_k \alpha^k$, qui est un élément de $\mathbb{K}$ appelé *évaluation de P en α*.
- La fonction $\alpha \longmapsto P(\alpha)$ de $\mathbb{K}$ dans $\mathbb{K}$ est appelée la *fonction polynomiale associée à P*.
  On la note souvent P par abus† et parfois $\widetilde{P}$ lorsque l'on veut la distinguer proprement du polynôme P.
- Pour tous $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$, $\widetilde{\lambda P + \mu Q} = \lambda \widetilde{P} + \mu \widetilde{Q}$, $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$ et $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.
- Pour tous $P, Q \in \mathbb{R}[X]$, $\widetilde{P'} = \widetilde{P}'$.

Démonstration. Admis. ∎

Les résultats des deux derniers points n'ont rien d'évidents a priori. Nous disposons sur $\mathbb{R}[X]$ et $\mathbb{R}^{\mathbb{R}}$ de notions DIFFÉRENTES d'addition, multiplication, composition et dérivation. Par exemple, dans la formule « $\widetilde{P'} = \widetilde{P}'$ », la dérivée P' est une dérivée formelle (celle de la définition 24), alors que la dérivée $\widetilde{P}'$ est la dérivée d'une fonction définie comme limite d'un taux d'accroissement.

✖ **ATTENTION !** ✖ $\boxed{X \text{ n'est pas un nombre !}}$
On ne dit pas « Posons $X = \alpha$ », mais « Évaluons en α » ou « Substituons X par α ».

Remarque 31 Puisque $\widetilde{1}$ est la fonction constante $x \longmapsto 1$, *i.e.* le neutre pour la multiplicaton de l'anneau $\mathbb{K}^{\mathbb{K}}$, l'application $P \longmapsto \widetilde{P}$ s'avère être un morphisme d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}^{\mathbb{K}}$.

Remarque 32 – Algorithme de Horner L'*algorithme de Horner*‡ permet de calculer l'évaluation en α d'un polynôme $P = \sum_{k=0}^{n} a_k X^k$ de degré n pour un coût de n additions et n multiplications dans $\mathbb{K}$ (l'algorithme naïf nécessitant $2n$ multiplications), en remarquant que

$$P(\alpha) = a_0 + \alpha(a_1 + \alpha(a_2 + \ldots + \alpha(a_{n-2} + \alpha(a_{n-1} + \alpha a_n))\ldots)).$$

Soit l'algorithme simple suivant :
- $S \leftarrow a_n$;
- Pour k allant de $n-1$ à 0 par pas de -1 : $S \leftarrow a_k + \alpha * S$.

Théorème 33 – Formule de Taylor§ polynomiale

Pour tout $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$,

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k.$$

En particulier, pour tout $k \in \mathbb{N}$, le coefficient de degré k de P est $\dfrac{P^{(k)}(0)}{k!}$.

Démonstration. ... ∎

†. Cette identification sera justifiée au chapitre 17.
‡. William George Horner (1786 à Bristol – 1837 à Bath) est un mathématicien britannique connu pour ladite méthode. À vrai dire, celle-ci était déjà employée par Isaac Newton 150 ans plus tôt et avait été exposée dès le 14e siècle par le mathématicien chinois Zhū Shìjié (le *fan fa*).
§. Brook Taylor (1685 à Edmonton – 1731 à Londres) est un mathématicien anglais à l'origine des développements qui portent aujourd'hui son nom et de la formule d'intégration par partie.

Remarque 34 Malgré les apparences, la somme $\displaystyle\sum_{k=0}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$ est finie, puisque $P^{(k)}$ est nul dès que $k > \deg P$.

4.2 Polynôme annulateur d'une matrice carrée

La structure d'anneau de l'ensemble $\mathscr{M}_n(\mathbb{K})$ permet d'évaluer un polynôme à coefficients dans $\mathbb{K}$ en une matrice carrée à coefficients dans $\mathbb{K}$. Précisément, pour tous $P = \displaystyle\sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$ et $A \in \mathscr{M}_n(\mathbb{K})$, on pose

$$P(A) = \sum_{k=0}^{+\infty} a_k A^k = a_p A^p + a_{p-1}A^{p-1} + \ldots + a_1 A + a_0 I_n,$$

pour tout $p > \deg P$. On vérifie alors sans difficulté, pour tous $P, Q \in \mathbb{K}[X]$, $\lambda, \mu \in \mathbb{K}$ et $A \in \mathscr{M}_n(\mathbb{K})$, les propriétés suivantes :

$$(\lambda P + \mu Q)(A) = \lambda P(A) + \mu Q(A) \qquad \text{et} \qquad (PQ)(A) = P(A)Q(A) = Q(A)P(A).$$

Définition 35 – Polynôme annulateur d'une matrice carrée

Soit $A \in \mathscr{M}_n(\mathbb{K})$. Un polynôme $P \in \mathbb{K}[X]$ est appelé UN *polynôme annulateur de la matrice* A lorsque $P(A) = 0_n$.

Exemple 36 Le polynôme $X^3 - 2X^2 - 1$ annule la matrice $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.
En effet, il suffit de vérifier que $A^3 - 2A^2 - I_3 = 0_3$.

Exemple 37 Pour tout $A \in \mathscr{M}_2(\mathbb{K})$, $X^2 - \operatorname{tr}(A)X + \det(A)$ est un polynôme annulateur de A.

Théorème 38 – Polynômes annulateurs et matrice inversible

Soit $A \in \mathscr{M}_n(\mathbb{K})$. Si A possède un polynôme annulateur de coefficient constant non nul, alors A est inversible.

Démonstration. ... ∎

Exemple 39 La matrice A de l'exemple 36 est inversible d'inverse $A^2 - 2A$.
En effet, étant annulée par $X^3 - 2X^2 - 1$, on a $A\big(A^2 - 2A\big) = A^3 - 2A^2 = I_3$.

Compétences à acquérir

- Utiliser la formule donnant les coefficients d'un produit de polynôme : exercices 2 et 5.
- Déterminer le degré d'un polynôme : exercices 3, 4 et 12.
- Manipuler les compositions de polynôme : exercice 9.
- Manipuler les dérivées de polynômes : exercices 7 à 9.

Quelques résultats classiques :

- Une formule de Vandermonde (application 10).
- Algorithme de Horner (remarque 32).
- Polynôme annulateur d'une matrice carrée de taille 2 (exemple 37).
- Degré du polynôme $P(X+1) - P(X)$ (exercice 4).
- Polynômes de Tchebychev (exercice 12, questions 1 et 3).